PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G09C 5/00, H04L 9/00 — A1

(11) International Publication Number: WO 98/02864

(43) International Publication Date: 22 January 1998 (22.01.98)

(21) International Application Number: PCT/US97/11455

(22) International Filing Date: 2 July 1997 (02.07.97)

(30) Priority Data:
08/677,435 2 July 1996 (02.07.96) US

(71) Applicant: THE DICE COMPANY [US/US]; Townhouse 4, 20191 E. Country Club Drive, Aventura, FL 33180 (US).

(72) Inventors: MOSKOWITZ, Scott, A.; Townhouse 4, 20191 E. Country Club Drive, Aventura, FL 33180 (US). COOPERMAN, Marc, S.; 2929 Ramona, Palo Alto, CA 94306 (US).

(74) Agents: ALTMILLER, John, C. et al.; Kenyon & Kenyon, 1025 Connecticut Avenue, N.W., Washington, DC 20036 (US).

(81) Designated States: AU, BR, CN, JP, Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: OPTIMIZATION METHODS FOR THE INSERTION, PROTECTION AND DETECTION OF DIGITAL WATERMARKS IN DIGITIZED DATA

(57) Abstract

The implementations of digital watermarks can be optimally suited to particular transmission, distribution and storage mediums given the nature of digitally-sampled audio, video and other multimedia works. Watermark application parameters can be adapted to the individual characteristics of a given digital sample stream. Watermark information can be either carried in individual samples or in relationships between multiple samples, such as in a waveform shape. More optimal models may be obtained to design watermark systems that are tamper-resistant given the number and breadth of existent digitized sample options with different frequency and time components. The highest quality of a given content signal may be maintained as it is mastered, with the watermark suitably hidden, taking into account usage of digital filters and error correction. The quality of the underlying content signals can be used to identify and highlight advantageous locations for the insertion of digital watermarks. The watermark is integrated as closely as possible to the content signal, at a maximum level to force degradation of the content signal when attempts are made to remove the watermarks.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

OPTIMIZATION METHODS FOR THE INSERTION, PROTECTION AND DETECTION OF DIGITAL WATERMARKS IN DIGITIZED DATA

RELATED APPLICATIONS

This application is related to patent applications entitled "Steganographic Method and Device", Serial No. 08/489,172 filed on June 7, 1995; "Method for Human-Assisted Random Key Generation and Application for Digital Watermark System", Serial No. 08/587,944 filed on January 17, 1996; "Method for Stega-Cipher Protection of Computer Code", Serial No. 08/587,943 filed on January 17, 1996; "Digital Information Commodities Exchange", Serial No. 08/365,454 filed on December 28, 1994, which is a continuation of Serial No. 08/083,593 filed on June 30, 1993; and "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management", Serial No. 08/674,726 filed on July 2, 1996. These related applications are all incorporated herein by reference.

This application is also related to U.S. Patent No. 5,428,606, "Digital Information Commodities Exchange", issued on June 27, 1995, which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

The present invention relates to digital watermarks.

Digital watermarks exist at a convergence point where creators and publishers of digitized multimedia content demand localized, secured

identification and authentication of that content. Because existence of piracy is clearly a disincentive to the digital distribution of copyrighted works, establishment of responsibility for copies and derivative copies of such works is invaluable. In considering the various forms of multimedia content, whether "master," stereo, NTSC video, audio tape or compact disc, tolerance of quality degradation will vary with individuals and affect the underlying commercial and aesthetic value of the content. It is desirable to tie copyrights, ownership rights, purchaser information or some combination of these and related data to the content in such a manner that the content must undergo damage, and therefore a reduction in value, with subsequent, unauthorized distribution of the content, whether it be commercial or otherwise.

Legal recognition and attitude shifts, which recognize the importance of digital watermarks as a necessary component of commercially distributed content (audio, video, game, etc.), will further the development of acceptable parameters for the exchange of such content by the various parties engaged in the commercial distribution of digital content. These parties may include artists, engineers, studios, INTERNET access providers, publishers, agents, on-line service providers, aggregators of content for various forms of delivery, on-line retailers, individuals and parties that participate in the transfer of funds to arbitrate the actual delivery of content to intended parties.

Since the characteristics of digital recordings vary widely, it is a worthwhile goal to provide tools to describe an optimized envelope of parameters for inserting, protecting and detecting digital watermarks in a given digitized sample (audio, video, virtual reality, etc.) stream. The optimization techniques described hereinafter make unauthorized removal of digital watermarks containing these parameters a significantly costly operation in terms of the absolute given projected economic gain from undetected commercial distribution. The optimization techniques, at the least, require significant damage to the content signal, as to make the

unauthorized copy commercially worthless, if the digital watermark is removed, absent the use of extremely expensive tools.

Presumably, the commercial value of some works will dictate some level of piracy not detectable in practice and deemed "reasonable" by rights holders given the overall economic return. For example, there will always be fake $100 bills, LEVI jeans, and GUCCI bags, given the sizes of the overall markets and potential economic returns for pirates in these markets--as there also will be unauthorized copies of works of music, operating systems (Windows95, etc.), video and future multimedia goods.

However, what differentiates the "digital marketplace" from the physical marketplace is the absence of any scheme that establishes responsibility and trust in the authenticity of goods. For physical products, corporations and governments mark the goods and monitor manufacturing capacity and sales to estimate loss from piracy. There also exist reinforcing mechanisms, including legal, electronic, and informational campaigns to better educate consumers.

SUMMARY OF THE INVENTION

The present invention relates to implementations of digital watermarks that are optimally suited to particular transmission, distribution and storage mediums given the nature of digitally-sampled audio, video, and other multimedia works.

The present invention also relates to adapting watermark application parameters to the individual characteristics of a given digital sample stream.

The present invention additionally relates to the implementation of digital watermarks that are feature-based. That is, a system where watermark information is not carried in individual samples, but is carried in the relationships between multiple samples, such as in a waveform shape. The present invention envisions natural extensions for digital watermarks that may also separate frequencies (color or audio), channels in 3D while utilizing discreteness in feature-based encoding only known to those with

pseudo-random keys (i.e., cryptographic keys) or possibly tools to access such information, which may one day exist on a quantum level.

The present invention additionally relates to a method for obtaining more optimal models to design watermark systems that are tamper-resistant given the number and breadth of existent digitized-sample options with differing frequency and time components (audio, video, pictures, multimedia, virtual reality, etc.).

To accomplish these goals, the present invention maintains the highest quality of a given content signal as it was mastered, with its watermarks suitably hidden, taking into account usage of digital filters and error correction presently concerned solely with the quality of content signals.

The present invention additionally preserves quality of underlying content signals, while using methods for quantifying this quality to identify and highlight advantageous locations for the insertion of digital watermarks.

The present invention integrates the watermark, an information signal, as closely as possible to the content signal, at a maximal level, to force degradation of the content signal when attempts are made to remove the watermarks.

The present invention relates to a method for amplitude independent encoding of digital watermark information in a signal including steps of determining in the signal a sample window having a minimum and a maximum, determining a quantization interval of the sample window, normalizing the sample window, normalizing the sample window to provide normalized samples, analyzing the normalized samples, comparing the normalized samples to message bits, adjusting the quantization level of the sample window to correspond to the message bit when a bit conflicts with the quantization level and de-normalizing the analyzed samples.

The present invention also relates to a method for amplitude independent decoding of digital watermark information in a signal including steps of determining in the signal a sample window having a minimum and a

maximum, determining a quantization interval of the sample window, normalizing the sample window to provide samples, and analyzing the quantization level of the samples to determine a message bit value.

The present invention additionally relates to a method of encoding and decoding watermarks in a signal where, rather than individual samples, insertion and detection of abstract signal features to carry watermark information in the signal is done.

The present invention also relates to a method for pre-analyzing a digital signal for encoding digital watermarks using an optimal digital filter in which it is determined what noise elements in the digital signal will be removed by the optimal digital filter based on response characteristics of the filter.

The present invention also relates to a method of error coding watermark message certificates using cross-interleaved codes which use error codes of high redundancy, including codes with Hamming distances of greater than or equal to "n", wherein "n" is a number of bits in a message block.

The present invention additionally relates to a method of pre-processing a watermark message certificate including a step of determining an absolute bit length of the watermark message as it will be encoded.

The present invention additionally relates to a method of generating watermark pseudo-random key bits using a non-linear (chaotic) generator or to a method of mapping pseudo-random key and processing state information to affect an encode/decode map using a non-linear (chaotic) generator.

The present invention additionally relates to a method of guaranteeing watermark certificate uniqueness including a step of attaching a time stamp or user identification dependent hash or message digest of watermark certificate data to the certificate.

The present invention also relates to a method of generating and quantizing a local noise signal to contain watermark information where the

noise signal is a function of at least one variable which depends on key and processing state information.

The present invention also relates to a method of dithering watermark quantizations such that the dither changes an absolute quantization value, but does not change a quantization level or information carried in the quantization.

The present invention further relates to a method of encoding watermarks including inverting at least one watermark bit stream and encoding a watermark including the inverted watermark bit stream.

The present invention also relates to a method of decoding watermarks by considering an original watermark synchronization marker, an inverted watermark synchronization marker, and inverted watermarks, and decoding based on those considerations.

The present invention also relates to a method of encoding and decoding watermarks in a signal using a spread spectrum technique to encode or decode where information is encoded or decoded at audible levels and randomized over both frequency and time.

The present invention additionally relates to a method of analyzing composite digitized signals for watermarks including obtaining a composite signal, obtaining an unwatermarked sample signal, time aligning the unwatermarked sample signal to the composite signal, gain adjusting the time aligned unwatermarked sample signal to the composite signal, estimating a pre-composite signal using the composite signal and the gain adjusted unwatermarked sample signal, estimating a watermarked sample signal by subtracting the estimated pre-composite signal for the composite signal, and scanning the estimated watermark sample signal for watermarks.

The present invention additionally relates to a method for varying watermark encode/decode algorithms automatically during the encoding or decoding of a watermark including steps of (a) assigning a list of desired CODECs to a list of corresponding signal characteristics which indicate use

of particular CODECs, (b) during encoding/decoding, analyzing characteristics of the current sample frame in the signal stream, prior to delivering the frame to CODEC, (c) looking up the corresponding CODEC from the list of CODECs in step (a) which matches the observed signal characteristics from step (b), (d) loading and/or preparing the desired CODEC, (e) passing the sample frame to the CODEC selected in step (c), and f) receiving the output samples from step (e).

The present invention also relates to a method for varying watermark encode/decode algorithms automatically during the encoding or decoding of a watermark, including steps of (a) assigning a list of desired CODECs to a list of index values which correspond to values computed to values computed as a function of the pseudo-random watermark key and the state of the processing framework, (b) during encoding/decoding, computing the pseudo-random key index value for the current sample frame in the signal stream, prior to delivering the frame to a CODEC, (c) looking up the corresponding CODEC from the list of CODECs in step (a) which matches the index value from step (b), (d) loading and/or preparing the desired CODEC, (e) passing the sample frame to the CODEC selected in step (c), and (f) receiving the output samples from step (e).

DETAILED DESCRIPTION

The present invention relates to implementations of digital watermarks that are optimally suited to particular transmission, distribution and storage mediums given the nature of digitally sampled audio, video, and other multimedia works.

The present invention also relates to adapting watermark application parameters to the individual characteristics of a given digital sample stream.

The present invention additionally relates to the implementation of digital watermarks that are feature-based. That is, a system where watermark information is not carried in individual samples, but is carried in the relationships between multiple samples, such as in a waveform shape.

For example, in the same manner a US $100 bill has copy protection features including ink type, paper stock, fiber, angles of artwork that distort in photocopier machines, inserted magnetic strips, and composite art, the present invention envisions natural extensions for digital watermarks that may also separate frequencies (color or audio), channels in 3D while utilizing discreteness in feature-based encoding only known to those with pseudo-random keys (i.e., cryptographic keys) or possibly tools to access such information, which may one day exist on a quantum level.

There are a number of hardware and software approaches in the prior art that attempt to provide protection of multimedia content, including encryption, cryptographic containers, cryptographic envelopes or "cryptolopes", and trusted systems in general. None of these systems places control of copy protection in the hands of the content creator as the content is created, nor provides an economically feasible model for exchanging the content to be exchanged with identification data embedded within the content.

Yet, given the existence of over 100 million personal computers and many more non-copy-protected consumer electronic goods, copy protection seems to belong within the signals. After all, the playing (i.e., using) of the content establishes its commercial value.

Generally, encryption and cryptographic containers serve copyright holders as a means to protect data in transit between a publisher or distributor and the purchaser of the data (i.e., a means of securing the delivery of copyrighted material from one location to another by using variations of public key cryptography or other more centralized cryptosystems).

Cryptolopes are suited specifically for copyrighted text that is time-sensitive, such as newspapers, where intellectual property rights and origin data are made a permanent part of the file. For information on public-key cryptosystems see U.S. Patent No. 4,200,770 to Hellman et al., U.S. Patent No. 4,218,582 to Hellman et al., U.S. Patent No. 4,405,829 to Rivest et al.,

and U.S. Patent No. 4,424,414 to Hellman et al. Systems are proposed by IBM and Electronic Publishing Resources to accomplish cryptographic container security.

Digitally-sampled copyrighted material, that is binary data on a fundamental level, is a special case because of its long term value coupled with the ease and perfectness of copying and transmission by general purpose computing and telecommunications devices. In particular, in digitally-sampled material, there is no loss of quality in copies and no identifiable differences between one copy and any other subsequent copy. For creators of content, distribution costs may be minimized with electronic transmission of copyrighted works. Unfortunately, seeking some form of informational or commercial return via electronic exchange is ill-advised absent the use of digital watermarks to establish responsibility for specific copies and unauthorized copying. Absent digital watermarks, the unlikely instance of a market of trusted parties who report any distribution or exchange of unauthorized copies of the protected work must be relied upon for enforcement. Simply, content creators still cannot independently verify watermarks should they choose to do so.

For a discussion of systems that are oriented around content-based addresses and directories, see U.S. Patent No. 5,428,606 to Moskowitz.

In combining steganographic methods for insertion of information identifying the title, copyright holder, pricing, distribution path, licensed owner of a particular copy, or a myriad of other related information, with pseudo-random keys (which map insertion location of the information) similar to those used in cryptographic applications, randomly placed signals (digital watermarks) can be encoded as random noise in a content signal. Optimal planning of digital watermark insertion can be based on the inversion of optimal digital filters to establish or map areas comprising a given content signal insertion envelope. Taken further, planning operations will vary for different digitized content: audio, video, multimedia, virtual reality, etc. Optimization techniques for processes are described in the

copending related applications entitled "Steganographic Method and Device" and "Method for Human Assisted Random Key Generation and Application for Digital Watermark System".

Optimization processes must take into consideration the general art of digitization systems where sampling and quantizing are fundamental physical parameters. For instance, discrete time sampling has a natural limit if packets of time are used, estimated at $1x10^{-42}$ second. This provides a natural limit to the sampling operation. Also, since noise is preferable to distortion, quantizing will vary given different storage mediums (magnetic, optical, etc.) or transmission mediums (copper, fiber optic, satellite, etc.) for given digitized samples (audio, video, etc.). Reducing random bit error, quantization error, burst error, and the like is done for the singular goal of preserving quality in a given digitized sample. Theoretical perfect error correction is not efficient, given the requirement of a huge allocation of redundant data to detect and correct errors. In the absence of such overhead, all error correction is still based on data redundancy and requires the following operations: error detection to check data validity, error correction to replace erroneous data, and error concealment to hide large errors or substitute data for insufficient data correction. Even with perfect error correction, the goal of a workable digital watermark system for the protection of copyrights would be to distribute copies that are less than perfect but not perceivably different from the original. Ironically, in the present distribution of multimedia, this is the approach taken by content creators when faced with such distribution mechanisms as the INTERNET. As an example, for audio clips commercially exchanged on the World Wide Web (WWW), a part of the INTERNET, 8 bit sampled audio or audio downsampled from 44.1 kHz (CD-quality), to 22 kHz and lower. Digital filters, however, are not ideal because of trade-offs between attenuation and time-domain response, but provide the engineer or similarly-trained individual with a set of decisions to make about maximizing content quality with minimum data overhead and consideration of the ultimate delivery

mechanism for the content (CDs, cable television, satellite, audio tape, stereo amplifier, etc.).

For audio signals and more generally for other frequency-based content, such as video, one method of using digital filters is to include the use of an input filter to prevent frequency aliasing higher than the so-called Nyquist frequencies. The Nyquist theorem specifies that the sampling frequency must be at least twice the highest signal frequency of the sampled information (e.g., for the case of audio, human perception of audio frequencies is in a range between 20 Hz and 20 kHz). Without an input filter, aliases can still occur leaving an aliased signal in the original bandwidth that cannot be removed.

Even with anti-aliasing filters, quantization error can still cause low level aliasing which may be removed with a dither technique. Dither is a method of adding random noise to the signal, and is used to de-correlate quantization error from the signal while reducing the audibility of the remaining noise. Distortion may be removed, but at the cost of adding more noise to the filtered output signal. An important effect is the subsequent randomization of the quantization error while still leaving an envelope of an unremovable signaling band of noise. Thus, dither is done at low signal levels, effecting only the least significant bits of the samples. Conversely, digital watermarks, which are essentially randomly-mapped noise, are intended to be inserted into samples of digitized content in a manner such as to maximize encoding levels while minimizing any perceivable artifacts that would indicate their presence or allow for removal by filters, and without destroying the content signal. Further, digital watermarks should be inserted with processes that necessitate random searching in the content signal for watermarks if an attacker lacks the keys. Attempts to over-encode noise into known watermarked signal locations to eliminate the information signal can be made difficult or impossible without damaging the content signal by relying on temporal encoding and randomization in the generation of keys during digital watermark insertion. As a result, although the

watermark occupies only a small percentage of the signal, an attacker is forced to over-encode the entire signal at the highest encoding level, which creates audible artifacts.

The present invention relates to methods for obtaining more optimal models to design watermark systems that are tamper-resistant given the number and breadth of existent digitized sample options with differing frequency and time components (audio, video, pictures, multimedia, virtual reality, etc.).

To accomplish these goals, the present invention maintains the highest quality of a given content signal as it was mastered, with its watermarks suitably hidden, taking into account usage of digital filters and error correction presently concerned solely with the quality of content signals.

Additionally, where a watermark location is determined in a random or pseudo-random operation dependent on the creation of a pseudo-random key, as described in copending related application entitled "Steganographic Method and Device" assigned to the present assignee, and unlike other forms of manipulating digitized sample streams to improve quality or encode known frequency ranges, an engineer seeking to provide high levels of protection of copyrights, ownership, etc. is concerned with the size of a given key, the size of the watermark message and the most suitable area and method of insertion. Robustness is improved through highly redundant error correction codes and interleaving, including codes known generally as q-ary Bose-Chaudhuri-Hocquenghem (BCH) codes, a subset of Hamming coding operations, and codes combining error correction and interleaving, such as the Cross-Interleave Reed-Solomon Code. Using such codes to store watermark information in the signal increases the number of changes required to obliterate a given watermark. Preprocessing the certificate by considering error correction and the introduction of random data to make watermark discovery more difficult, prior to watermarking, will help determine sufficient key size. More generally, absolute key size can be

determined through preprocessing the message and the actual digital watermark (a file including information regarding the copyright owner, publisher, or some other party in the chain of exchange of the content) to compute the absolute encoded bit stream and limiting or adjusting the key size parameter to optimize the usage of key bits. The number of bits in the primary key should match or exceed the number of bits in the watermark message, to prevent redundant usage of key bits. Optimally, the number of bits in the primary key should exactly match the watermark size, since any extra bits are wasted computation.

Insertion of informational signals into content signals and ranges from applications that originate in spread spectrum techniques have been contemplated. More detailed discussions are included in copending related applications entitled "Steganographic Method and Device" and entitled "Method for Human Assisted Random Key Generation and Application for Digital Watermark System".

The following discussion illustrates some previously disclosed systems and their weaknesses.

Typically, previously disclosed systems lack emphasis or implementation of any pseudo-random operations to determine the insertion location, or map, of information signals relating to the watermarks. Instead, previous implementations provide "copy protect" flags in obvious, apparent and easily removable locations. Further, previous implementations do not emphasize the alteration of the content signal upon removal of the copy protection.

Standards for digital audio tape (DAT) prescribe insertion of data such as ISRC (Industry Standard Recording Codes) codes, title, and time in sub-code according to the Serial Copy Management System (SCMS) to prevent multiple copying of the content. One time copying is permitted, however, and systems with AES3 connectors, which essentially override copy protection in the sub-code as implemented by SCMS, actually have no copy limitations. The present invention provides improvement over this

implementation with regard to the ability of unscrupulous users to load digital data into unprotected systems, such general computing devices, that may store the audio clip in a generalized file format to be distributed over an on-line system for further duplication. The security of SCMS (Serial Copy Management System) can only exist as far as the support of similarly-oriented hardware and the lack of attempts by those skilled in the art to simply remove the subcode data in question.

Previous methods seek to protect content, but shortcomings are apparent. U.S. Patent No. 5,319,735 to Preuss et al. discusses a spread spectrum method that would allow for over-encoding of the described, thus known, frequency range and is severely limited in the amount of data that can be encoded-- 4.3 8-bit symbols per second. However, with the Preuss et al. method, randomization attacks will not result in audible artifacts in the carrier signal, or degradation of the content as the information signal is in the subaudible range. It is important to note the difference in application between spread spectrum in military field use for protection of real-time radio signals, and encoding information into static audio files. In the protection of real-time communications, spread spectrum has anti-jam features, since information is sent over several channels at once. Therefore, in order to jam the signal, one has to jam all channels, including their own. In a static audio file, however, an attacker has practically unlimited time and processing power to randomize each sub-channel in the signaling band without penalty to themselves, so the anti-jam advantages of spread spectrum do not extend to this domain.

In a completely different implementation, U.S. Patent No. 5,379,345 to Greenberg seeks enforcement of broadcast contracts using a spread spectrum modulator to insert signals that are then confirmed by a spread spectrum-capable receiver to establish the timing and length that a given, marked advertisement is played. This information is measured against a specific master of the underlying broadcast material. The Greenberg patent does not ensure that real-time downloads of copyrighted content can be

marked with identification information unless all download access points (PCs, modems, etc.), and upload points for that matter, have spread spectrum devices for monitoring.

Other methods include techniques similar to those disclosed in related copending patent applications mentioned above by the present assignee, but lack the pseudo-random dimension of those patent applications for securing the location of the signals inserted into the content. One implementation conducted by Michael Gerzon and Peter Craven, and described by Ken Pohlmann in the 3rd edition of Principles of Digital Audio, illustrates a technology called "buried data technique," but does not address the importance of randomness in establishing the insertion locations of the informational signals in a given content signal, as no pseudo-random methods are used as a basis for insertion. The overriding concern of the "buried data techniques" appears to be to provide for a "known channel" to be inserted in such a manner as to leave little or no perceivable artifacts in the content signal while prescribing the exact location of the information (i.e., replacing the least significant bits (LSB) in a given information signal). In Gerzon and Craven's example, a 20-bit signal gives way to 4-bits of LSBs for adding about 27 dB of noise to the music. Per channel data insertion reached 176.4 kilobits per second per channel, or 352.8 kbps with stereo channels. Similarly attempted data insertion by the present inventors using random data insertion yielded similar rates. The described techniques may be invaluable to manufacturers seeking to support improvements in audio, video and multimedia quality improvements. These include multiple audio channel support, surround sound, compressed information on dynamic range, or any combination of these and similar data to improve quality. Unfortunately, this does little or nothing to protect the interests of copyright holders from unscrupulous pirates, as they attempt to create unmarked, perfect copies of copyrighted works.

The present invention also relates to copending patent applications

entitled "Staganographicc Method and Device"; "Method for Human-Assisted Random Key Generation and Application for Digital Watermark System"; and "Method for Stega-Cipher Protection of Computer Code" as mentioned above, specifically addressing the weakness of inserting informational signals or digital watermarks into known locations or known frequency ranges, which are sub-audible. The present invention seeks to improve on the methods disclosed in these patent applications and other methods by describing specific optimization techniques at the disposal of those skilled in the art. These techniques provide an a la carte method for rethinking error correction, interleaving, digital and analog filters, noise shaping, nonlinear random location mapping in digitized samples, hashing, or making unique individual watermarks, localized noise signal mimic encoding to defeat noise filtering over the entire sample stream, super audible spread spectrum techniques, watermark inversion, preanalyzing watermark key noise signatures, and derivative analysis of suspect samples against original masters to evaluate the existence of watermarks with statistical techniques.

The goal of a digital watermark system is to insert a given information signal or signals in such a manner as to leave few or no artifacts in the underlying content signal, while maximizing its encoding level and location sensitivity in the signal to force damage to the content signal when removal is attempted. The present invention establishes methods for estimating and utilizing parameters, given principles of the digitization of multimedia content (audio, video, virtual reality, etc.), to create an optimized "envelope" for insertion of watermarks, and thus establish secured responsibility for digitally sampled content. The pseudo-random key that is generated is the only map to access the information signal while not compromising the quality of the content. A digital watermark naturally resists attempts at removal because it exists as purely random or pseudo-random noise in a given digitized sample. At the same time, inversion techniques and mimicking operations, as well as encoding signal features instead of given

samples, can make the removal of each and every unique encoded watermark in a given content signal economically infeasible (given the potential commercial returns of the life of a given copyright) or impossible without significantly degrading the quality of the underlying, "protected" signal. Lacking this aesthetic quality, the marketability or commercial value of the copy is correspondingly reduced.

The present invention preserves quality of underlying content signals, while using methods for quantifying this quality to identify and highlight advantageous locations for the insertion of digital watermarks.

The present invention integrates the watermark, an information signal, as closely as possible to the content signal, at a maximal level, to force degradation of the content signal when attempts are made to remove the watermarks.

General methods for watermarking digitized content, as well as computer code, are described in copending related patent applications entitled "Steganographic Method and Device" and entitled "Method for Stega-Cipher Protection of Computer Code", both assigned to the present assignee. Recognizing the importance of perceptual encoding of watermarks by the authors and engineers who actually create content is addressed in copending related application entitled "Method for Human Assisted Random Key Generation and Application for Digital Watermark System".

The present invention describes methods of random noise creation given the necessary consequence of improving signal quality with digitization techniques. Additionally, methods are described for optimizing projections of data redundancy and overhead in error correction methods to better define and generate parameters by which a watermarking system can successfully create random keys and watermark messages that subsequently cannot be located and erased without possession of the key that acts as the map for finding each encoded watermark. This description will provide the backdrop for establishing truly optimized watermark

insertion including: use of nonlinear (chaotic) generators; error correction and data redundancy analysis to establish a system for optimizing key and watermark message length; and more general issues regarding desired quality relating to the importance of subjecting watermarked content to different models when the content may be distributed or sold in a number of prerecorded media formats or transmitted via different electronic transmission systems; this includes the use of perceptual coding; particularized methods such as noise shaping; evaluating watermark noise signatures for predictability; localized noise function mimic encoding; encoding signal features; randomizing time to sample encoding of watermarks; and, finally, a statistical method for analyzing composite watermarked content against a master sample content to allow watermark recovery. All of these features can be incorporated into specialized digital signal processing microprocessors to apply watermarks to nongeneralized computing devices, such as set-top boxes, video recorders that require time stamping or authentication, digital video disc (DVD) machines and a multitude of other mechanisms that play or record copyrighted content.

The sampling theorem, known specifically as the Nyquist Theorem, proves that bandlimited signals can be sampled, stored, processed, transmitted, reconstructed, desampled or processed as discrete values. In order for the theorem to hold true, the sampling must be done at a frequency that is at least twice the frequency of the highest signal frequency to be captured and reproduced. Aliasing will occur as a form of signal fold over, if the signal contains components above the Nyquist frequency. To establish the highest possible quality in a digital signal, aliasing is prevented by low-pass filtering the input signal to a given digitization system by a low-pass or anti-aliasing filter. Any residue aliasing which may result in signal distortion, relates to another area of signal quality control, namely, quantization error removal.

Quantization is required in a digitization system. Because of the continuous nature of an analog signal (amplitude vs. time), a quantized

sample of the signal is an imperfect estimate of the signal sample used to encode it as a series of discrete integers. These numbers are merely estimates of the true value of the signal amplitude. The difference between the true analog value at a discrete time and the quantization value is the quantization error. The more bits allowed per sample, the greater the accuracy of estimation; however, errors still always will occur. It is the recurrent nature of quantization errors that provides an analogy with the location of digital watermarks.

Thus, methods for removal of quantization errors have relevance in methods for determining the most secure locations for placement of watermarks to prevent the removal of such watermarks.

The highest fidelity in digital reproduction of a signal occurs at points where the analog signal converges with a given quantization interval. Where there is no such convergence, in varying degrees, the quantization error will be represented by the following range:

+Q /2 and -Q/2, where Q is the quantization interval.

Indeed, describing maximization of the quantization error and its ratio with the maximum signal amplitude, as measured, will yield a signal-to-error ratio (S/E) which is closely related to the analog signal-to-noise ratio (S/N). To establish more precise boundaries for determining the S/E, with root mean square (rms) quantization error E_{rms}, and assuming a uniform probability density function 1/Q (amplitude), the following describes the error:

$$E_{rms}=Q/(12)^{½}$$

Signal to quantization error is expressed as:

$$S/E=[S_{rms}/E_{rms}]^2=3/2(2^{2n})$$

Finally, in decibels (dB) and comparing 16-bit and 15-bit quantization:

$$S/E(dB)=10\log[3/2(2^{2n})]=10\log 3/2+2^n\log 2$$

(or "= 20log $[(3/2)^{½}(2^n)]$")

$$=6.02n+1.76$$

This explains the S/E ratio of 98 dB for 16-bit and 92 dB for 15-bit quantization. The 1.76 factor is established statistically as a result of peak-to-rms ratio of a sinusoidal waveform, but the factor will differ if the signal waveform differs. In complex audio signals, any distortion will exist as white noise across the audible range. Low amplitude signals may alternatively suffer from distortion.

Quantization distortion is directly related with the original signal and is thus contained in the output signal, it is not simply an error. This being the case, implementation of so-called quality control of the signal must use dither. As discussed above, dither is a method of adding random noise to the signal to de-correlate quantization error from the signal while reducing the audibility of the remaining noise. Distortion may be removed at the cost of adding more noise to the filtered output signal. An important effect is the subsequent randomization of the quantization error while still leaving an envelope of an unremovable signaling band of noise. Dither, done at low signal levels, effects only the least significant bits of the samples.

Use of linear and nonlinear quantization can effect the trade-off in the output signal and must be considered for a system of watermarks designed to determine acceptable quantization distortion to contain the digital watermark. For audio systems, block linear quantization implementations have been chosen. However, block floating point and floating point systems, nonuniform companding, adaptive delta modulation, adaptive differential pulse-code modulation, and perceptual coding schemes (which are oriented around the design of filters that closely match the actual perception of humans) appear to provide alternative method implementations that would cause higher perceptible noise artifacts if filtering for watermarks was undertaken by pirates. The choice of method is related to the information overhead desired.

According to one aspect of the present invention, the envelope described in the quantization equations above is suitable for preanalysis of a digitized sample to evaluate optimal locations for watermarks. The

present example is for audio, but corresponding applications for digitization of video would be apparent in the quantization of color frequencies.

The matter of dither complicates preanalysis of a sample evaluated for digital watermarks. Therefore, the present invention also defines the optimal envelope more closely given the three types of dither (this example is for audio, others exist for video): triangular probability density function (pdf), Gaussian pdf, and rectangular pdf. Again, to establish better boundaries for the random or pseudo-random insertion of a watermark to exist in a region of a content signal that would represent an area for hiding watermarks in a manner most likely to cause damage to the content signal if unauthorized searches or removal are undertaken. Dither makes removal of quantization error more economical through lower data overhead in a system by shifting the signal range to decorrelate errors from the underlying signal. When dither is used, the dither noise and signal are quantized together to randomize the error. Dither which is subtractive requires removing the dither signal after requantization and creates total error statistical independence. It would also provide further parameters for digital watermark insertion given the ultimate removal of the dither signal before finalizing the production of the content signal. With nonsubtractive dither, the dither signal is permanently left in the content signal. Errors would not be independent between samples. For this reason, further analysis with the three types of dither should reveal an acceptable dither signal without materially affecting the signal quality.

Some proposed systems for implementing copyright protection into digitally-sampled content, such as that proposed by Digimarc Corporation, predicate the natural occurrence of artifacts that cannot be removed. Methods for creating a digital signature in the minimized error that is evident, as demonstrated by explanations of dither, point out another significant improvement over the art in the system described in the present invention and its antecedents. Every attempt is made to raise the error level of error from LSBs to a level at which erasure necessarily leads to the

degradation of the "protected" content signal. Furthermore, with such a system, pirates are forced to make guesses, and then changes, at a high enough encoding level over a maximum amount of the content signal so as to cause signal degradation, because guessing naturally introduces error. Thus, dither affects the present invention's envelope by establishing a minimum encoding level. Any encoding done below the dither level might be erased by the dither.

One embodiment of the present invention may be viewed as the provision of a random-super-level non-subtractive dither which contains information (the digital watermark).

To facilitate understanding of how this does not cause audible artifacts, consider the meaning of such encoding in terms of the S/E ratio. In a normal 16-bit signal, there is a 98 dB S/E according to the equation S/E = 6.02n + 1.76. Consider that the encoding of watermark information looks like any other error, except it moves beyond the quantization level, out of the LSBs. If the error is of a magnitude expressed in, say, 8 bits, then at that moment, the signal effectively drops to 8 bits (16-8). This corresponds to a momentary drop in S/E, referred to herein as the momentary S/E. Yet, these errors are relatively few and far between and therefore, since the signal is otherwise comprised of higher-bit samples, a "Perceived S/E" may be derived which is simply the weighted average of the samples using the "Pure S/E" (the samples without watermark information) and those with the Momentary S/E. As a direct consequence, it may be observed that the more sparse the watermark map, the fewer errors introduced in a given range, and the higher the perceived S/E. It also helps that the error is random, and so over time, appears as white noise, which is relatively unobtrusive. In general, it is observed that as long as introduced errors leave resulting samples within an envelope in the sample window described by minimum and maximum values, before error introduction, and the map is sufficiently sparse, the effects are not perceived.

In addition, it is possible to obtain an even higher Perceived S/E by allowing the range of introduced errors to vary between a minimum and maximum amount. This makes the weighted average S/E higher by reducing the average introduced error level. Yet, someone trying to erase a watermark, assuming they knew the maximum level, would have to erase at that level throughout the data, since they would not know how the introduced level varies randomly, and would want to erase all watermarks.

A watermarking cipher could perform this operation and may also introduce the further step of local dither (or other noise) significantly above the quantization amplitude on a window by window basis randomly, to restrict total correlation between the watermark signal and the probability that it remains independent between samples, as with subtractive dither implementations that are mostly concerned with the ultimate removal of the dither signal with requantization. This ability could be used to accomplish signal doping, which adds a degree of random errors that do not contain watermark information so as to prevent differential analysis of multiple watermarked copies. Alternatively, it could be used to mimic a specific noise function in a segment of the signal in order to defeat attempts to filter a particular type of noise over the entire signal. By varying this function between watermarks, it may be guaranteed that any particular filter is of no use over the whole signal. By applying several filters in series, it seems intuitive that the net results would be significantly different from the original signal.

The discussion may be more appropriately introduced with perceptual coding techniques, but a watermarking system could also defeat some detection and correction with dither by inserting watermarks into signal features, instead of signal samples. This would be equivalent to looking for signal characteristics, independent of the overall sample as it exists as a composite of a number of signals. Basically, instead of encoding on a bit per sample basis, one might spread bits over several samples. The point of doing this is that filtering and convolution operations, like "flanging", which

definitely change individual samples on a large scale, might leave intact enough of a recognizable overall signal structure (the relationship between multiple samples) to preserve the watermark information. This may be done by measuring, generalizing, and altering features determined by the relationships between samples or frequency bands. Because quantization is strictly an art of approximation, signal-to-error ratios, and thus the dynamic range of a given system are determined.

The choice of eliminating quantization distortion at the expense of leaving artifacts (not perceptible) is a permanent trade-off evident in all digitization systems which are necessarily based on approximation (the design goal of the present invention in preanalyzing a signal to mask the digital watermarks make imperceptibility possible). The high fidelity of duplication and thus subsequent ability to digitally or electronically transmit the finished content (signal) is favored by consumers and artists alike. Moreover, where there continues to be a question of approximating in quantization-- digital watermark systems will have a natural partner in seeking optimized envelopes in the multitude and variety of created digitized content.

Another aspect of optimizing the insertion of digital watermarks regards error correction. Highly redundant error codes and interleaving might create a buffer against burst errors introduced into digital watermarks through randomization attacks. A detailed description follows from the nature of a digitization system-- binary data can be corrected or concealed when errors exist. Random bit errors and burst errors differ in their occurrence:

Random bit errors are error bits occurring in a random manner, whereas burst errors may exist over large sequences of the binary data comprising a digitized signal. Outside the scope of the present invention are errors caused by physical objects, such as dust and fingerprints, that contribute to the creation of dropouts are different from the errors addressed herein.

Measuring error with bit-error ratio (BER), block error ratio (BLER) and burst-error length (BERL), however, provides the basis of error correction. Redundancy of data is a focus of the present invention. This data necessarily relies on existing data, the underlying content. To efficiently describe optimal parameters for generating a cryptographic key and the digital watermark message discussion of error correction and error concealment techniques is important.

Forms of error detection include one-bit parity, relying on the mathematical ability to cast out numbers, for binary systems including digitization systems, such as 2. Remainders given odd or even results (parity) that are probablistically determined to be errors in the data. For more appropriate error detection algorithms, such as Cyclic Redundancy Check Code (CRCC), which are suited for the detection of commonly occurring burst error. Pohlmann (Principles of Digital Audio) notes the high accuracy of CRCC (99.99%) and the truth of the following statements given a k-bit data word with m bits of CRCC, a code word of n bits is formed (m=n-k):

- burst errors less than or equal to m bits are always predictable.
- the detection probability of burst errors of m+1 bits = $1-2^{-m+1}$.
- the detection probability of burst errors longer than m+1 bits = $1-2^{-m}$
- random errors up to 3 consecutive bits long can be detected.

The medium of content delivery, however, provides the ultimate floor for CRCC design and the remainder of the error correction system.

Error correction techniques can be broken into three categories: methods for algebraic block codes, probablistic methods for convolutional codes, and cross-interleave code where block codes are used in a convolution structure. As previously discussed, the general class of codes that assist in pointing out the location of error are known generally as Hamming codes, versus CRCC which is a linear block code.

What is important for establishing parameters for determining optimized error coding in systems such as digital audio are more specifically known as Reed-Solomon Codes which are effective methods for correcting burst errors. Certain embodiments of the present invention presuppose the necessity of highly redundant error codes and interleaving, such as that done in Cross Interleave Reed-Solomon Code, to counter burst errors typically resulting from randomization attacks. More generally, certain embodiments of the present invention include the use of Hamming Codes of (n,n) to provide n-1 bit error detection and n-2 bit error correction. Further, a Hamming distance of n (or greater than n) is significant because of the nature of randomization attacks. Such an attack seeks to randomize the bits of the watermark message. A bit can be either 0 or 1, so any random change has a 50% chance of actually changing a bit from what it was (50% is indicative of perfect randomness). Therefore, one must assume that a good attack will change approximately half the bits (50%). A Hamming distance of n or greater, affords redundancy on a close par with such randomization. In other words, even if half the bits are changed, it would still be possible to recover the message.

Because interleaving and parity makes data robust for error avoidance, certain embodiments of the present invention seek to perform time interleaving to randomly boost momentary S/E ratio and give a better estimate of not removing keys and watermarks that may be subsequently determined to be "errors."

Given a particular digital content signal, parity, interleaving, delay, and cross-interleaving, used for error correction, should be taken into account when preprocessing information to compute absolute size requirements of the encoded bit stream and limiting or adjusting key size parameters to optimize and perhaps further randomize usage of key bits. In addition, these techniques minimize the impact of errors and are thus valuable in creating robust watermarks.

Uncorrected errors can be concealed in digital systems. Concealment offers a different dynamic to establish insertion parameters for the present invention. Error concealment techniques exist because it is generally more economical to hide some errors instead of requiring overly expensive encoders and decoders and huge information overheads in digitization systems. Muting, interpolation, and methods for signal restoration (removal of noise) relate to methods suggested by the present invention to invert some percentage or number of watermarks so as to ensure that at least some or as many as half of the watermarks must still remain in the content signal to effectively eliminate the other half. Given that a recording contains noise, whether due to watermarks or not, a restoration which "removes" such noise is likely to result in the changing of some bit of the watermark message. Therefore, by inverting every other watermark, it is possible to insure that the very act of such corrections inverts enough watermark bits to create an inverse watermark. This inversion presupposes that the optimized watermark insertion is not truly optimal, given the will of a determined pirate to remove watermarks from particularly valuable content. Ultimately, the inability to resell or openly trade unwatermarked content will help enforce, as well as dictate, the necessity of watermarked content for legal transactions.

The mechanisms discussed above reach physical limits as the intent of signal filtering and error correction are ultimately determined to be effective by humans-- decidedly analog creatures. All output devices are thus also analog for playback.

The present invention allows for a preprocessed and preanalyzed signal stream and watermark data to be computed to describe an optimized envelope for the insertion of digital watermarks and creation of a pseudo-random key, for a given digitized sample stream. Randomizing the time variable in evaluating discrete sample frames of the content signal to introduce another aspect of randomization could further the successful insertion of a watermark. More importantly, aspects of perceptual coding

are suitable for methods of digital watermarks or super-audible spread spectrum techniques that improve on the art described by the Preuss et al. patent described above.

The basis for a perceptual coding system, for audio, is psychoacoustics and the analysis of only what the human ear is able to perceive. Similar analysis is conducted for video systems, and some may argue abused, with such approaches as "subliminal seduction" in advertising campaigns. Using the human for design goals is vastly different than describing mathematical or theoretical parameters for watermarks. On some level of digital watermark technology, the two approaches may actually complement each other and provide for a truly optimized model.

The following example applies to audio applications. However, this example and other examples provided herein are relevant to video systems as well as audio systems. Where a human ear can discern between energy inside and outside the "critical band," (described by Harvey Fletcher) masking can be achieved. This is particularly important as quantization noise can be made imperceptible with perceptual coders given the maintenance of a sampling frequency, decreased word length (data) based on signaling conditions. This is contrasted with the necessary decrease of 6 dB/bit with decreases in the sampling frequency as described above in the explanation of the Nyquist Theorem. Indeed, data quantity can be reduced by 75%. This is an extremely important variable to feed into the preprocessor that evaluates the signal in advance of "imprinting" the digital watermark.

In multichannel systems, such as MPEG-1, AC-3 and other compression schemes, the data requirement (bits) is proportional to the square root of the number of channels. What is accomplished is masking that is nonexistent perceptually, only acoustically.

Taken to another level for digital watermarking, which is necessary for content that may be compressed and decompressed, forward adaptive

allocation of bits and backward adaptive allocation provide for encoding signals into content signals in a manner such that information can be conveyed in the transmission of a given content signal that is subsequently decoded to convey the relatively same audible signal to a signal that carries all of its bits-- e.g., no perceptual differences between two signals that differ in bit size. This coding technique must also be preanalyzed to determine the most likely sample bits, or signal components, that will exist in the smaller sized signal. This is also clearly a means to remove digital watermarks placed into LSBs, especially when they do not contribute theoretically perceptible value to the analyzed signal. Further methods for data reduction coding are similarly important for preanalyzing a given content signal prior to watermarking. Frequency domain coders such as subband and transform bands can achieve data reduction of ratios between 4:1 and 12:1. The coders adaptively quantize samples in each subband based on the masking threshold in that subband (See Pohlmann, Principles of Digital Audio). Transform coders, however, convert time domain samples into the frequency domain for accomplishing lossless compression. Hybrid coders combine both subband and transform coding, again with the ultimate goal of reducing the overall amount of data in a given content signal without loss of perceptible quality.

With digital watermarks, descriptive analysis of an information signal is important to preanalyze a given watermark's noise signature. Analysis of this signature versus the preanalysis of the target content signal for optimized insertion location and key/message length, are potentially important components to the overall implementation of a secure watermark. It is important that the noise signature of a digital watermark be unpredictable without the pseudo-random key used to encode it. Noise shaping, thus, has important applications in the implementation of the present invention. In fact, adaptive dither signals can be designed to correlate with a signal so as to mask the additional noise-- in this case a digital watermark. This relates to the above discussion of buried data

techniques and becomes independently important for digital watermark systems. Each instance of a watermark, where many are added to a given content signal given the size of the content and the size of the watermark message, can be "noise shaped" and the binary description of the watermark signature may be made unique by "hashing" the data that comprises the watermark. Generally, hashing the watermark certificate prior to insertion is recommended to establish differences between the data in each and every watermark "file."

Additionally, the present invention provides a framework in which to analyze a composite content signal that is suspected to contain a watermarked sample of a copyrighted work, against an unwatermarked original master of the same sample to determine if the composite content actually contains a copy of a previously watermarked content signal. Such an analysis may be accomplished in the following scenario:

- Assume the composite signal contains a watermark from the sample.

- Assume the provision of the suspect composite signal $C_w(t)$ (w subscript denotes a possible watermark) and the unwatermarked original sample $S_{uw}(t)$. These are the only two recordings the analyzer is likely to have access to.

Now, it is necessary to recover a watermarked sample $S_w(t)$.

The methods of digital signal processing allow for the computation of an optimal estimate of a signal. The signal to be estimated is the composite minus the watermarked sample, or $C"_w(t) = C_w(t) - S_w(t)$. The analyzer, however, cannot determine a value of $S_w(t)$, since it does not know which of the many possible $S_w(t)$ signals was used in the composite. However, a close estimate may be obtained by using $S_{uw}(t)$, since watermarking makes relatively minor changes to a signal.

So, $C"_w(t)$ (an estimate of $C'_w(t)$ given $C_w(t)$ and $S_{uw}(t)$) may be obtained. Once $C"_w(t)$ is calculated, it is simply subtracted from $C_w(t)$. This yields $S'_w(t) = C_w(t) - C"_w(t)$. If the watermark is robust enough, and the estimate good enough,

then $S'_w(t)$, which is approximately equal to $S_w(t)$, can be processed to extract the watermark. It is simply a matter of attempting watermark decoding against a set of likely encoding key candidates.

Note that although a watermark is initially suspected to be present in the composite, and the process as if it is, the specifics of the watermark are not known, and a watermark is never introduced into the calculations, so a watermark is extracted, it is valid, since it was not introduced by the signal processing operations.

The usefulness of this type of operation is demonstrated in the following scenario:

People are interested in simply proving that their copyrighted sample was dubbed into another recording, not the specifics of ownership of the sample used in the dubbing. So, this implies that only a single, or limited number of watermark keys would be used to mark samples, and hence, the decode key candidates are limited, since the same key would be used to encode simple copyright information which never varies from copy to copy.

There are some problems to solve to accomplish this sort of processing. The sample in question is generally of shorter duration than the composite, and its amplitude may be different from the original. Analysis techniques could use a combination of human-assisted alignment in the time domain, where graphical frequency analysis can indicate the temporal location of a signal which closely matches that of the original sample. In addition, automatic time warping algorithms which time align separate signals, on the assumption they are similar could also be used to solve temporal problems. Finally, once temporal alignment is accomplished, automatic amplitude adjustment could be performed on the original sample to provide an optimal match between the composite section containing the sample and the original sample.

It may be desirable to dynamically vary the encoding/decoding algorithm during the course of encoding/decoding a signal stream with a given watermark. There are two reasons for dynamically varying the encoding/decoding algorithm.

The first reason for dynamically varying the encoding/decoding algorithm is that the characteristics of the signal stream may change between one locality in the stream and another locality in the stream in a way that significantly changes the effects that a given encoding algorithm may have on the perception of that section of the stream on playback. In other words, one may want the encoding algorithm, and by implication, the decoding algorithm, to adapt to changes in the signal stream characteristics that cause relative changes in the effects of the encoding algorithm, so that the encoding process as a whole causes fewer artifacts, while maintaining a certain level of security or encoding a given amount of information.

The second reason for dynamically varying the encoding/decoding algorithm is simply to make more difficult attempts at decoding watermarks without keys. It is obviously a more difficult job to attempt such attacks if the encoding algorithm has been varied. This would require the attacker to guess the correct order in which to use various decoding algorithms.

In addition, other reasons for varying the encoding/decoding algorithms may arise in the future.

Two methods for varying of the encoding/decoding algorithms according to embodiments of the present invention are described herein. The first method corresponded to adaptation to changing signal characteristics. This method requires a continuous analysis of the sample windows comprising the signal stream as passed to the framework. Based on these characteristics, which are mathematically well-defined functions of the sample stream (such as RMS energy, RMS/peak ratio, RMS difference between samples - which could reflect a measure of distortion), a new CODEC module, from among a list of pre-defined CODECs, and the algorithms implemented in them, can be applied to the window in question. For the purpose of this discussion, windows are assumed to be equivalent to frames. And, in a frame-based system, this is a straightforward application of the architecture to provide automated variance of algorithms to encode and decode a single watermark.

The second method for varying of the encoding/decoding algorithms corresponds to increased security. This method is easier, since it does not require the relatively computationally-expensive process of further analyzing the samples in a frame passed to the Framework. In this method, the Framework selects a new CODEC, from among a list of pre-defined CODECs, to which to pass the sample frame as a function of the pseudo-random key employed to encode/decode the watermark. Again, this is a straightforward application of framework architecture which provides automated variance of algorithms to encode and decode a single watermark versus limitations evident in the analysis of a single random noise signal inserted over the entire content signal as proposed by Digimarc, NEC, Thorn EMI and IBM under the general guise of spread spectrum, embedded signalling schemes.

It is important to note that the modular framework architecture, in which various modules including CODECs are linked to keys, provides a basic method by which the user can manually accomplish such algorithmic variations for independent watermarks. The main difference detailed above is that an automated method to accomplish this can be used within single watermarks.

Automated analysis of composited copyrighted material offers obvious advantages over subjective "human listening" and "human viewing" methods currently used in copyright infringement cases pursued in the courts.

What Is Claimed Is:

1. A method for amplitude independent encoding of digital watermark information in a signal, comprising steps of:

determining in said signal a sample window having a minimum and a maximum;

determining a quantization interval of said sample window, where said quantitization interval can be used to quantize normalized window samples;

normalizing the sample window to provide normalized samples, where normalized samples conform to a limited range of values, proportional to real sample values, and comprise a representation of the real sample values with a resolution higher than the real range of values, and where the normalized values can be divided by the quantization interval into distinct quantization levels;

analyzing the normalized samples to determine quantization levels;

comparing the message bits to the corresponding quantization level information from the analyzing step;

when a bit conflicts with the quantization level, adjusting the quantization level of said sample window to correspond to the message bit; and

de-normalizing the analyzed normalized samples.

2. The method according to claim 1, wherein watermark signal characteristics or a watermark certificate can be compressed.

3. A method for amplitude independent decoding of digital watermark information in a signal comprising steps of:

determining in said signal a sample window having a minimum and a maximum;

determining a quantization interval of said sample window, where said quantitization interval can be used to quantize normalized window samples;

normalizing the sample window to provide samples, where normalized samples conform to a limited range of values, proportional to real sample values, and comprise a representation of the real sample values with a resolution higher than the real range of values, and where the normalized values can be divided by the quantization interval into distinct quantization levels; and

analyzing the quantization level of said samples to determine a message bit value.

4. The method according to claim 3, wherein watermark signal characteristics or a watermark certificate can be compressed.

5. A method of encoding and decoding watermarks in a signal, comprising insertion and detection of abstract signal features in said signal to carry watermark information, wherein said abstract signal features are mathematical functions of the input sample window, and by extension, adjacent sample windows.

6. A method of pre-analyzing a digital signal for encoding digital watermarks using a digital filter comprising determining what changes in the digital signal will be affected by the digital filter.

7. The method according to claim 6, further comprising a step of encoding watermarks so as to either avoid frequency or time delimited areas of the signal which will be changed by the digital filter, or ensure that the watermark will survive the changes instroduced by the digital filter.

8. A method of error coding watermark message certificates using cross interleaved codes which use error codes of high redundancy, including codes with Hamming distances of greater than or equal to n, wherein is a number of bits in a message block.

9. A method of pre-processing a watermark message certificate comprising determining an exact length of the watermark message as it will be encoded.

10. The method according to claim 9, further comprising a step of generating a watermark key which will provide at least one unique bit for each bit comprising the watermark message.

11. A method of generating watermark pseudo-random key bits using a non-linear generator.

12. A method of generating watermark pseudo-random key bits using a chaotic generator.

13. A method of mapping pseudo-random key and processing state information to effect an encode / decode map using a non-linear generator.

14. A method of mapping pseudo-random key and processing state information to effect an encode / decode map using a chaotic generator.

15. A method of guaranteeing watermark certificate uniqueness comprising attaching a timestamp or user identification dependent hash or message digest of watermark certificate data to the certificate.

16. A method of generating and modulating a local noise signal to contain watermark information, wherein the noise signal is a function of at least one variable which depends on key and processing state information.

17. A method of dithering watermark quantizations such that the dither changes an absolute quantization value, but does not change a quantization level or information carried in the quantization.

18. A method of encoding watermarks comprising steps of:

inverting at least one instance of the watermark bit stream; and

encoding at least one instance of the watermark using said inverted instance of the watermark bit stream.

19. A method of decoding watermarks comprising steps of:

considering an original watermark synchronization marker, an inverted watermark synchronization marker, and inverted watermarks; and

decoding based on the considering step.

20. A method of encoding and decoding watermarks in a signal using a spread spectrum technique to encode or decode where information is encoded or decoded at audible levels and the encoding and decoding methods are pseudo-random over frequency.

21. A method of encoding and decoding watermarks in a signal using a spread spectrum technique to encode or decode where information is encoded or decoded at audible levels and the encoding and decoding methods are pseudo-random over time.

22. The method of claim 21, wherein the information is encoded or decoded at audible levels and the encoding and decoding methods are pseudo-random, over both frequency and time.

23. A method of analyzing composite digitized signals for watermarks comprising steps of:

obtaining a composite signal;

obtaining an unwatermarked sample signal;

time aligning the unwatermarked sample signal to the composite signal;

gain adjusting the time aligned unwatermarked sample signal to a corresponding segment of the composite signal, determined in the time aligning step;

estimating a pre-composite signal using the composite signal and the gain adjusted unwatermarked sample signal;

estimating a watermarked sample signal by subtracting the estimated pre-composite signal from the composite signal; and

scanning the estimated watermarked sample signal for watermarks.

24. A method for varying watermark encode/decode algorithms automatically during the encoding or decoding of a watermark comprising steps of:

a) assigning a list of desired CODECs to a list of corresponding signal characteristics which indicate use of particular CODECs;

b) during encoding/decoding, analyzing characteristics of the current sample frame in the signal stream, prior to delivering the frame to a CODEC;

c) looking up the corresponding CODEC from the list of CODECs in step (a) which matches the observed signal characteristics from step (b);

d) loading and/or preparing the desired CODEC;

e) passing the sample frame to the CODEC selected in step (c); and

f) receiving the output samples from step (e).

25. The method according to claim 24, wherein watermark signal characteristics or a watermark certificate can be compressed.

26. A method for varying watermark encode/decode algorithms automatically during the encoding or decoding of a watermark comprising steps of:

a) assigning a list of desired CODECs to a list of index values which correspond to values computed as a function of the pseudo-random watermark key and the state of the processing framework;

b) during encoding/decoding, computing the pseudo-random key index value for the current sample frame in the signal stream, prior to delivering the frame to a CODEC;

c) looking up the corresponding CODEC from the list of CODECs in step (a) which matches the index value from step (b);

d) loading and/or preparing the desired CODEC;

e) passing the sample frame to the CODEC selected in step (c); and

f) receiving the output samples from step (e).

27. The method according to claim 26, wherein watermark signal characteristics or a watermark certificate can be compressed.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/11455

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G09C 5/00 H04L 9/00

US CL :380/54, 3, 4, 23, 55; 283/73, 113, 17

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/54, 3, 4, 23, 55, 49, 51, 59; 283/73, 113, 17

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, E	US 5,664,018 A (LEIGHTON) 02 SEPTEMBER 1997	1-27
A, P	US, 5,636,292 A (RHOADS) 03 JUNE 1997	1-27
A, P	US 5,617,119 A (BRIGGS ET AL.) 01 APRIL 1997	1-27
A, P	US 5,568,570 A (RABBANI) 22 OCTOBER 1996	1-27
A, P	US 5,530,759 A (BRAUDAWAY, ET AL.) 25 JUNE 1996	1-27
A	US 5,493,677 A (BALOGH, ET AL.) 20 FEBRUARY 1996	1-27

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
23 OCTOBER 1997

Date of mailing of the international search report
23 DEC 1997

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
DAVID CAIN
Telephone No. (703) 305-1836

Form PCT/ISA/210 (second sheet)(July 1992)★